Statement of
James B. Comey
Deputy Attorney General
United States Department of Justice
Before the
Committee on the Judiciary
United States House of Representatives

June 8, 2005

Introduction

Good Morning. Chairman Sensenbrenner, Ranking Member Conyers and Members of the Committee, it is my pleasure to appear before you today to discuss the USA PATRIOT Act. Thank you for allowing me the opportunity to discuss the important tools contained in that Act. As I have said many times before Members and Committees of both houses of Congress, and all over the country, when it comes to the USA PATRIOT Act, I believe that the angel is in the details and that if we engage in conversation and shed daylight on how the Department of Justice has used the important tools in the Act, more people will come to see that the tools are simple, constitutional, and just plain sensible.

The Administration is fighting the War against Terror both at home and abroad using all the lawful tools at our disposal. Survival and success in this struggle demand that the Department continuously improve its capabilities to protect Americans from a relentless enemy. The Department will continue to seek the assistance of Congress as it builds a culture of prevention and ensures that our government's resources are dedicated to defending the safety and security of the American people.

I will never forget, as I know the Members of this Committee will not forget, the thousands of our fellow citizens that were murdered at the World Trade Center, the Pentagon and a field in rural Pennsylvania. Nearly four years have passed since that tragic day and, in large part due to the tremendous efforts of our federal, state and local law enforcement as well as the Intelligence Community, our country has been spared another attack of that magnitude. But our success presents a new challenge. How do we bring voice to victims that were never murdered, to family members who have not lost a loved one? How do we explain to Congress and the American people these "ghost pains?" This is the continuing challenge of law enforcement in our country. When we are faced with rising crime and victimization rates, it is easy to point to those in need of our protection to justify our requests for tools to protect our citizens. But when we are successful in our efforts, when our hard work and relentlessness pays off, it becomes more difficult to convince the people to let us keep those tools.

Mr. Chairman, as a career prosecutor, and now in my role as Deputy Attorney General, I have heard many times the question of when will we next break up a terror cell moments before implementation of a devastating plot. But let me tell you, as a prosecutor, you don't want to be there. You want to catch a terrorist with his hands on the check instead of his hands on the bomb. You want to be many steps ahead of the devastating event. The way we do that is

through preventive and disruptive measures, by using investigative tools to learn as much as we can as quickly as we can and then incapacitating a target at the right moment. Tools such as enhanced information sharing mechanisms, roving surveillance, pen registers, requests for the production of business records, and delayed notification search warrants allow us to do just that.

Proactive prosecution of terrorism-related targets on less serious charges is often an effective method of deterring and disrupting potential terrorist planning and support activities. Moreover, guilty pleas to these less serious charges often lead defendants to cooperate and provide information to the Government information that can lead to the detection of other terrorism-related activity.

I'd next like to discuss the material support statutes, which are the cornerstone of our prosecution efforts. The first material support case to be tried before a jury involved a group of Hizballah operatives in Charlotte, North Carolina found to have been involved in a massive inter-state cigarette smuggling and tax evasion scheme. The investigation uncovered a related plot in which some of these defendants were procuring dual-use items at the instructions of Hizballah leaders in Lebanon. This indictment, which involved RICO and material support charges, resulted in the conviction of 20 people. The Charlotte prosecution was upheld by the Fourth Circuit Court of Appeals (*United States v. Hammoud*, 4th Cir., September 8, 2004; remanded for resentencing in light of *Booker*). Since then, "material support" charges have been used against other cigarette smuggling plots in Detroit. We have successfully prosecuted *al Qaeda* supporters in Portland and Alexandria, and Hizballah supporters in Detroit and Charlotte. We have convicted persons involved in *jihad* training activities in Buffalo, Seattle, and Alexandria.

Indeed, prior to the attacks of 9/11, 17 persons in four different judicial districts were charged with offenses relating to material support to terrorists and terrorist organizations. Since then, however, 135 people in at least 25 different judicial districts have been charged with material support-related offenses. Of the 152 people charged both before and since 9/11, 70 have been convicted or pleaded guilty, and many more are still awaiting trial.

Our prosecution of those who seek to provide material support continues including most recently a on April 27, 2005, a New Jersey federal jury convicted Hemant Lakhani, a United Kingdom national, of attempting to provide material support to terrorists for his role in trying to sell an antiaircraft missile to a man whom he believed represented a terrorist group intent on shooting down a United States commercial airliner. On April 22, 2005, in the Eastern District of Virginia, Zacarias Moussaoui pled guilty to six counts of conspiracy, acknowledging his role in assisting *al Qaeda*. Also on April 22, 2005, a jury convicted Ali Al-Timimi, a speaker and spiritual leader in Northern Virginia, in the second phase of the Northern Virginia jihad case involving a group of individuals who were encouraged and counseled by Al-Timimi to go to Pakistan to receive military training from Lashkar-e-Taiba, which has ties to the *al Qaeda* terrorist network, in order to be able to fight against American troops. The first phase of the

prosecution involved convictions under the material support statutes; Al-Timimi's firearms convictions were predicated, in part, on the material support statutes. And there are many more examples due to our continuing efforts to ensure the safety of the American people.

Foreign Intelligence Surveillance Act

The authorities contained in the Foreign Intelligence Surveillance Act (FISA) have been critical to the Department's efforts to combat terrorism. Since September 11, 2001, the volume of applications to the Foreign Intelligence Surveillance Court (FISA Court) has dramatically increased. In 2000, 1,012 applications for surveillance or searches were filed under FISA. By comparison, in 2004 we filed 1,758 applications; this represents a 74% increase in four years. Of the 1,758 applications made in 2004, none were denied, although 94 were modified by the FISA Court in some substantive way.

In enacting the USA PATRIOT Act and the Intelligence Reform and Terrorism Prevention Act of 2004, Congress provided the government with tools that it has used regularly and effectively in its war on terrorism. The reforms in those measures affect every single application made by the Department for electronic surveillance or physical searches authorized under FISA regarding suspected terrorists and have enabled the government to become quicker and more flexible in gathering critical intelligence information on suspected terrorists. It is because of the key importance of these tools to winning the war on terror that the Department asks you to reauthorize those USA PATRIOT Act provisions scheduled to expire at the end of this year.

For example, section 207 of the USA PATRIOT Act governs the authorized periods for FISA collection and has been essential to protecting both the national security of the United States and the civil liberties of Americans. It changed the time periods for which some electronic surveillance and physical searches are authorized under FISA, and, in doing so, conserved limited resources of both the FBI and the Department's Office of Intelligence Policy and Review (OIPR). Instead of devoting time to the mechanics of repeatedly renewing FISA applications in certain cases -- which are considerable -- those resources are now devoted to other investigative activities as well as conducting appropriate oversight of the use of intelligence collection authorities at the FBI and other intelligence agencies. A few examples of how section 207 has helped the Department are set forth below.

Since its inception, FISA has permitted electronic surveillance of an individual who is an agent of foreign power based upon his status as a non-United States person who acts in the United States as "an officer or employee of a foreign power, or as a member" of an international terrorist group. As originally enacted, FISA permitted electronic surveillance of such targets for initial periods of 90 days, with extensions for additional periods of up to 90 days based upon subsequent applications by the government. In addition, FISA originally allowed the

government to conduct physical searches of any agent of a foreign power (including United States persons) for initial periods of 45 days, with extensions for additional 45-day periods.

Section 207 of the USA PATRIOT Act changed the law to permit the government to conduct electronic surveillance and physical search of certain agents of foreign powers and non-resident-alien members of international groups for initial periods of 120 days, with extensions for periods of up to one year. It also allows the government to obtain authorization to conduct physical searches targeting any agent of a foreign power for periods of up to 90 days. Section 207 did not change the time periods applicable for electronic surveillance of United States persons, which remain at 90 days. By making these time periods for electronic surveillance and physical search equivalent, it has enabled the Department to file streamlined combined electronic surveillance and physical search applications that, in the past, were tried but abandoned as too cumbersome to do effectively.

As the Attorney General testified before the House Judiciary Committee, we estimate that the amendments in section 207 have saved OIPR approximately 60,000 hours of attorney time in the processing of FISA applications. This figure does not include the time saved by agents and attorneys at the FBI. Because of section 207's success, the Department has proposed additional amendments to increase the efficiency of the FISA process. Among these would be to allow initial coverage of any non-U.S. person agent of a foreign power for 120 days with each renewal of such authority allowing continued coverage for one year. Had this and other proposals been included in the USA PATRIOT Act, the Department estimates that an additional 25,000 attorney hours would have been saved in the interim. Most of these ideas were specifically endorsed in the recent report of the bipartisan WMD Commission. The WMD Commission agreed that these changes would allow the Department to focus its attention where it is most needed and to ensure adequate attention is given to cases implicating the civil liberties of Americans. Section 207 is scheduled to sunset at the end of this year.

Access to Tangible Things

Section 215 of the USA PATRIOT Act allows the FBI to obtain an order from the FISA Court requesting production of any tangible thing, such as business records, if the items are relevant to an ongoing authorized national security investigation, which, in the case of a United States person, cannot be based solely upon activities protected by the First Amendment to the Constitution. The Attorney General recently declassified the fact that the FISA Court has issued 35 orders requiring the production of tangible things under section 215 from the effective date of the Act through March 30th of this year. None of those orders were issued to libraries and/or booksellers, and none were for medical or gun records. The provision to date has been used only to order the production of driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses for telephone numbers captured through court-authorized pen register devices.

Similar to a prosecutor in a criminal case issuing a grand jury subpoena for an item relevant to his investigation, so too can an investigator obtain an order from the FISA Court requiring production of records or items that are relevant to an investigation to protect against international terrorism or clandestine intelligence activities. Section 215 orders, however, are subject to judicial oversight before they are issued – unlike grand jury subpoenas. The FISA Court must explicitly authorize the use of section 215 to obtain business records before the government may serve the order on a recipient. In contrast, grand jury subpoenas are subject to judicial review only if they are challenged by the recipient. Section 215 orders are also subject to a similar standard as are grand jury subpoenas – a relevance standard.

Section 215 has been criticized by some because it does not exempt libraries and booksellers. The absence of such an exemption is consistent with criminal investigative practice. Prosecutors have always been able to obtain records from libraries and bookstores through grand jury subpoenas. Libraries and booksellers should not become safe havens for terrorists and spies. Last year, a member of a terrorist group closely affiliated with *al Qaeda* used Internet service provided by a public library to communicate with his confederates. Furthermore, we know that spies have used public library computers to do research to further their espionage and to communicate with their co-conspirators. For example, Brian Regan, a former TRW employee working at the National Reconnaissance Office, who was convicted of espionage, extensively used computers at five public libraries in Northern Virginia and Maryland to access addresses for the embassies of certain foreign governments.

Concerns that section 215 allows the government to target Americans because of the books they read or websites they visit are misplaced. The provision explicitly prohibits the government from conducting an investigation of a U.S. person based solely upon protected First Amendment activity. 50 U.S.C. § 1861(a)(2)(B). And, as the Attorney General has made clear, we have no interest in the reading habits of ordinary Americans. However, some criticisms of section 215 have apparently been based on possible ambiguity in the law. The Department has already stated in litigation that the recipient of a section 215 order may consult with his attorney and may challenge that order in court. The Department has also stated that the government may seek, and a court may require, only the production of records that are relevant to a national security investigation, a standard similar to the relevance standard that applies to grand jury subpoenas in criminal cases. The text of section 215, however, is not as clear as it could be in these respects. The Department, therefore, would support amendments to section 215 to clarify these points. Section 215 also is scheduled to sunset at the end of this year.

The right of a recipient to challenge a production order must, however, be distinguished from a potential right of a third party to suppress information obtained from the recipient--a right not normally afforded in criminal proceedings. This, for example, is true in the case of grand jury subpoenas. *See, e.g., United States v. Miller*, 425 U.S. 435 (1976) (holding that bank customer had no standing to challenge the validity of grand jury subpoenas issued to a bank for

his records). Similarly, a defendant in a criminal proceeding has no constitutional right to suppress evidence obtained in a search of someone else's property, even if that search was conducted unlawfully. *See, e.g., Rakas v. Illinois*, 439 U.S. 128 (1978) (passengers in car have no standing to suppress evidence obtained in allegedly illegal search and seizure of car); *see also Wong Sun v. United States*, 371 U.S. 471 (1963) (defendant may not suppress evidence obtained as a product of statement made by co-defendant incident to an unlawful arrest, even though the evidence was inadmissible against co-defendant); *United States v. Mendoza-Burciaga*, 981 F.2d 192 (5th Cir. 1992) (driver of a truck has standing to challenge a search of the truck, but a passenger does not).

While the Department supports the aforementioned clarifying amendments to section 215, the Department is very concerned by proposals currently pending before Congress which would require the government to show "specific and articulable facts" that the records sought through a section 215 order pertain to a foreign power or agent of a foreign power. Such a requirement would disable the government from using a section 215 order at the early stages of an investigation, which is precisely when such an order is most useful.

Consider, for example, a case where a known terrorist is observed having dinner with an unknown individual at a hotel. Currently, investigators may use section 215 to obtain the unknown individual's hotel records so that he may be identified and then investigated further so that the government may find out if he is also involved in terrorism. It is important to remember that terrorists and spies are generally trained to camouflage their dangerous activities and thus even an innocent conversation or encounter may look benign to an untrained observer. But our agents must be enabled to, when conducting surveillance, follow up on individuals associating with known *al Qaeda* operatives. Such a use of section 215, however, would not be permissible if the standard were changed from relevance to one of specific and articulable facts that the records pertain to a foreign power or agent of a foreign power. This is because investigators in this hypothetical do not yet know whether the unknown individual is a terrorist or spy. Indeed, that is exactly the question that investigators are trying to answer by using section 215.

Pen Register and Trap-and-Trace Devices

Some of the most useful, and least intrusive, investigative tools available to both intelligence and law enforcement investigators are pen registers and trap and trace devices. These devices record data regarding incoming and outgoing communications, such as all of the telephone numbers that call, or are called by, certain phone numbers associated with a suspected terrorist or spy. These devices, however, are not used to record the substantive content of the communications. For that reason, the Supreme Court has held that there is no Fourth Amendment protected privacy interest in information acquired from telephone calls by a pen register. Nevertheless, information obtained by pen registers or trap and trace devices can be extremely useful in an investigation by revealing the nature and extent of the contacts between a

subject and his confederates. The data provides important leads for investigators, and may assist them in building the facts necessary to obtain probable cause to support a full content wiretap.

Under chapter 206 of title 18, which has been in place since 1986, if an FBI agent and prosecutor in a criminal investigation of a bank robber or an organized crime figure want to install and use pen registers or trap and trace devices, the prosecutor must file an application to do so with a federal court. The application they must file, however, is exceedingly simple: it need only specify the identity of the applicant and the law enforcement agency conducting the investigation, as well as "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." Such applications, of course, include other information about the facility that will be targeted and details about the implementation of the collection, as well as "a statement of the offense to which the information likely to be obtained . . . relates," but chapter 206 does not require an extended recitation of the facts of the case.

In contrast, prior to the USA PATRIOT Act, in order for an FBI agent conducting an intelligence investigation to obtain FISA authority to use the same pen register and trap and trace device to investigate a spy or a terrorist, the government was required to file a complicated application under title IV of FISA. Not only was the government's application required to include "a certification by the applicant that the information likely to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation being conducted by the Federal Bureau of Investigation under guidelines approved by the Attorney General," it also had to include the following:

> information which demonstrates that there is reason to believe that the telephone line to which the pen register or trap and trace device is to be attached, or the communication instrument or device to be covered by the pen register or trap and trace device, has been or is about to be used in communication with—
>
> > (A) an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States; or
> >
> > (B) a foreign power or agent of foreign power under circumstances giving reason to believe that the communication concerns or concerned international terrorism or clandestine intelligence activities that involve or may involve a violation of the criminal laws of the United States.

Thus, the government had to make a much different showing in order obtain a pen register or trap and trace authorization to find out information about a spy or a terrorist than is required to obtain the very same information about a drug dealer or other ordinary criminal. Sensibly, section 214 of the USA PATRIOT Act simplified the standard that the government

must meet in order to obtain pen/trap data in national security cases. Now, in order to obtain a national security pen/trap order, the applicant must certify "that the information likely to be obtained is foreign intelligence information not concerning a United States person, or is relevant to an investigation to protect against international terrorism or clandestine intelligence activities." Importantly, the law requires that such an investigation of a United States person may not be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Section 214 should not be permitted to expire and return us to the days when it was more difficult to obtain pen/trap authority in important national security cases than in normal criminal cases. This is especially true when the law already includes provisions that adequately protect the civil liberties of Americans. I therefore urge you to re-authorize section 214.

Proposals currently before the Congress would raise the standard for obtaining a pen register or trap and trace device – both in the criminal investigative and FISA contexts – from relevance to "specific and articulable facts." Like subpoenas, pen registers and trap and trace devices are not as intrusive as other investigative techniques and often are used as the building blocks of an investigation. Federal courts have held that the Constitution does not even require a court order for such a device to be installed (though federal statute does so require) because of the lower expectation of privacy that attaches to the numbers dialed to and from a telephone. Imposing a specific and articulable facts standard on pen registers/trap and trace devices would hamper investigations just as imposing such a standard on section 215 orders would.

Information Sharing

During the 1980s, the Department operated under a set of largely unwritten rules that limited to some degree information sharing between intelligence and law enforcement officials. In 1995, however, the Department established formal procedures that more clearly separated law enforcement and intelligence investigations and limited the sharing of information between intelligence and law enforcement personnel more than the law required. The promulgation of these procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overcome intelligence gathering as an investigation's primary purpose. To be sure, the procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers, while at the same time ensuring that the FBI would be able to obtain or continue FISA coverage and later use the fruits of that coverage in a criminal prosecution. Over time, however, coordination and information sharing between intelligence and law enforcement investigators became even more limited in practice than was allowed in theory under the Department's procedures. Due both to confusions about when sharing was permitted and to a perception that improper information sharing could end a career, a culture developed within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

Through enactment of sections 203 and 218, the USA PATRIOT Act helped bring down this "wall" separating intelligence officers from law enforcement agents. It not only erased the perceived statutory impediment to more robust information sharing between intelligence and law enforcement personnel, but it also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing.

The Department's efforts to increase coordination and information sharing between intelligence and law enforcement officers, which were made possible by the USA PATRIOT Act, have yielded extraordinary dividends by enabling the Department to open numerous criminal investigations, disrupt terrorist plots, bring numerous criminal charges, and convict numerous individuals in terrorism cases. For example, the removal of the barriers separating intelligence and law enforcement personnel played an important role in investigations and prosecutions of the Portland Seven, Sami Al-Arian, the Virginia Jihad case and numerous others.

Some have voiced the concern that under section 218 of the USA PATRIOT Act the government may utilize FISA surveillance when its primary purpose is to investigate and prosecute crimes unrelated to foreign intelligence. For example, the government, in obtaining a surveillance order targeting an agent of a foreign power, may have a significant purpose of obtaining foreign intelligence information but its primary purpose would be to investigate and prosecute that agent of a foreign power for a crime unrelated to foreign intelligence, such as tax fraud. This interpretation of FISA, however, has been clearly rejected by the FISA Court of Review, which observed that it would be "an anamolous reading" of section 218. The manifestation of such a primary purpose, the FISA Court of Review has stated, "would disqualify an application" under FISA. According to the court, this is because "the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes." *In re Sealed Case*, 310 F.3d 717, 736 (FISCR 2002).

Roving Wiretaps

Another important tool provided in the USA PATRIOT Act was provided by section 206, which allows the FISA Court to authorize "roving" surveillance of a terrorist or spy. This "roving" wiretap order attaches to a particular target rather than a particular phone or other communication facility. Since 1986, law enforcement has been able to use roving wiretaps to investigate ordinary crimes, including drug offenses and racketeering. Section 206 simply authorized the same techniques used to investigate ordinary crimes to be used in national security investigations. Before the USA PATRIOT Act, the use of roving wiretaps was not available under FISA. Therefore, each time a suspect changed communication providers, investigators had to return to the FISA Court for a new order just to change the name of the facility to be monitored and the "specified person" needed to assist in monitoring the wiretap. International terrorists and foreign intelligence officers are trained to thwart surveillance by

changing communication facilities just prior to important meetings or communications. This provision therefore has put investigators in a better position to counter the actions of spies and terrorists who are trained to thwart surveillance. This is a tool that we do not use often, but when we use it, it is critical. As of March 30, 2005, it had been used 49 times.

Section 206 also contains important privacy safeguards. Under Section 206, the target of roving surveillance must be identified or described in the order. Therefore, section 206 is always connected to a particular target of surveillance. Even if the government is not sure of the actual identify of the target of the wiretap, FISA nonetheless requires the government to provide "a description of the target of the electronic surveillance" to the FISA Court prior to obtaining a roving surveillance order. Under Section 206, furthermore, before approving a roving surveillance order, the FISA Court must find that there is probable cause to believe the target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or a spy. The description of the target must, therefore, be sufficiently detailed for the FISA Court to find probable cause that the target is either a foreign power or an agent of a foreign power. Roving surveillance under section 206 also can be ordered only after a FISA Court makes a finding that the actions of the target of the application may have the effect of thwarting the surveillance. Moreover, Section 206 in no way altered the FISA minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons. A number of federal courts, including the Second, Fifth, and Ninth Circuits, have squarely ruled that "roving" wiretaps are perfectly consistent with the Fourth Amendment. No court of appeals has reached a contrary conclusion.

Proposals currently pending before Congress would require the government to know the "identity" of the target in order to obtain a roving wiretap. This limitation would be problematic in the FISA context, in which we may be dealing with spies and terrorists trained to cloak their identities. If the government is able to find a description of the target sufficiently specific to allow the FISA Court to find probable cause that the target is an agent of a foreign power and may take action to thwart surveillance, the FISA Court should be able to authorize roving surveillance of that target.

Proposals in Congress also would require that the presence of the target at a particular telephone be "ascertained" by the person conducting the surveillance before the phone could be surveilled. This is a stricter standard than is required in the criminal context and would be impracticable in the FISA context, in which surveillance is usually done continually on a targeted phone and later translated and culled pursuant to minimization procedures. Moreover, such a requirement would be exceptionally risky in a world where terrorists and spies are trained extensively in counter-surveillance measures.

National Security Letters

Currently, NSLs, which are similar to administrative subpoenas, are issued for certain types of documents "relevant" to international terrorism or espionage investigations. Provisions currently before Congress would amend each existing NSL authority to impose one or more "specific and articulable facts" requirements. For each type of record, the government would be required to show specific and articulable facts that the records sought "pertain to a foreign power or agent of a foreign power." Additional specific and articulable facts requirements would be imposed with respect to other types of information. For example, with respect to telephone subscriber information, the government would have to show specific and articulable facts that the subscriber's communications devices "have been used" in communication with certain categories of individuals. These standards would significantly reduce the usefulness of NSLs for the same reason that a heightened standard of proof would diminish the usefulness of section 215.

Delayed Notification Search Warrants

Section 213 of the USA PATRIOT Act brought national uniformity to a court-approved law enforcement tool that had been in existence for decades and has been relied on by investigators and prosecutors in limited but essential circumstances. While there has been much discussion about this provision, there remain many misconceptions about this tool. The concept of rolling back delayed notification search warrants in any manner concerns me and demonstrates, I believe, a misunderstanding of how our criminal justice system works. Approval to delay notification of a search warrant is granted only after a federal judge finds reasonable cause to believe that immediate notification of execution of a search warrant would bring one of five enumerated adverse results including destruction of evidence, witness tampering, or serious jeopardy to an investigation. It is important to remember that judicial approval for the underlying search warrant is also required and remains governed by the probable cause standard. Nothing in the USA PATRIOT Act changed that. Also, notice is always provided to the target of the search, it is only delayed temporarily.

Section 213, like other provisions of the USA PATRIOT Act, is one tool we use in our efforts to combat terrorism. Although the Department has used this provision at least 18 times in terrorism-related investigations, it is true that this provision is used more frequently in non-terrorism contexts, particularly large, sensitive drug investigations, as it was for decades before the USA PATRIOT Act. This should not undermine the fact that it is an important tool to law enforcement and should not be limited to only the national security context. Indeed, the use of delayed notice search warrants in non-terrorism cases is consistent with Congressional intent – section 213 was never limited to terrorism cases. Some opponents of this tool also attempt to hold our agents' and prosecutors professionalism against us, by pointing to statistics showing that federal judges have never denied a request for a delayed notification search warrant. At the Department of Justice, we have the highest expectations for our professionals. Every prosecutor pushes for more than the bare minimum and takes great care to lay out facts and circumstances

in application for a search warrant that meet or exceed the probable cause requirement. In addition, the record reflects the fact that the Department has judiciously sought delayed notification search warrants as they comprise fewer than 2 in 1000 search warrants issued nationwide.

Some opponents of our use of section 213 would strike one essential justification for delayed notices search warrants, that immediate notice would "seriously jeopardize an investigation" from the statute. This would hamper criminal investigations in circumstances where immediate notice would cause an adverse effect not otherwise listed in the statute. For example, if the "seriously jeopardize" prong were eliminated, notice could not be delayed even if immediate notice of a search would jeopardize an ongoing and productive Title III wiretap. I'd like to highlight one example of where the "seriously jeopardizing an investigation" prong was the sole "adverse result" used to request delayed notice.

In 2004 the Justice Department executed three delayed notice searches as part of an OCDETF investigation of a major drug trafficking ring that operated in the Western and Northern Districts of Texas. The investigation lasted a little over a year and employed a wide variety of electronic surveillance techniques such as tracking devices and wiretaps of cell phones used by the leadership. The original delay approved by the court in this case was for 60 days. The Department sought two extensions, one for 60 days and one for 90 days, both of which were approved.

During the wiretaps, three delayed-notice search warrants were executed at the organization's stash houses. The search warrants were based primarily on evidence developed as a result of the wiretaps. Pursuant to section 213 of the USA PATRIOT Act, the court allowed the investigating agency to delay the notifications of these search warrants. Without the ability to delay notification, the Department would have faced two choices: (1) seize the drugs which would have alerted the criminals to the existence of wiretaps and thereby end our ability to build a significant case on the leadership or (2) not seize the drugs and allow the organization to continue to sell them in the community as we continued with the investigation. Because of the availability of delayed-notice search warrants, the Department was not forced to make this choice. Agents seized the drugs, continued this investigation, and listened to incriminating conversations as the dealers tried to figure out what had happened to their drugs.

On March 16, 2005, a grand jury returned an indictment charging twenty-one individuals with conspiracy to manufacture, distribute, and possess with intent to distribute more than 50 grams of cocaine base. Nineteen of the defendants, including all of the leadership, are in custody. All of the search warrants have been unsealed, and notice has been given in all cases.

In addition, certain proposals currently before Congress would limit the discretion of a federal judge in granting the initial periods of delay other than seven days. It would allow extensions in 21-day increments, but only if the Attorney General, DAG, or Associate Attorney

General personally approved the application for an extension. Requiring the government to go back to court after seven days – even where the court would have found a longer period of delay reasonable under the circumstances – would unduly burden law enforcement and judicial resources. And although the provision for a 21-day extension period is better than the 7-day period previously suggested by critics, requiring personal approval by the AG, DAG, or Associate would be impractical and unnecessarily burdensome. Currently, the length of delay is decided on a case-by-case basis by a federal judge familiar with the facts of a particular investigation. The Department believes that this system has worked well and should not be replaced by a one-size-fits-all statutory time limit.

Allegations of Abuse

In addition, the Department of Justice remains very concerned about any allegations of abuse of the tools provided in the USA PATRIOT Act. I am pleased that the Congress takes its oversight role seriously and has been attempting to address any relevant allegations. As Congress decides the fate of the tools contained in the Act, I hope that it does so in a thoughtful manner and in response to real concerns, not as a reaction to baseless allegations.

Recently, Senator Dianne Feinstein shared with the Department of Justice correspondence from the American Civil Liberties Union (ACLU). That correspondence was in response to her request for information regarding alleged "abuses" of the USA PATRIOT Act. Senator Feinstein requested that the Department review these allegations. Our review demonstrated that each matter cited by the ACLU either did not, in fact, involve the USA PATRIOT Act, or was an entirely appropriate use of the Act.

For example, the ACLU's letter alleged that the "Patriot Act [was used] to secretly search the home of Brandon Mayfield, a Muslim attorney whom the government wrongly suspected, accused and detained as a perpetrator of the Madrid train bombings." Mr. Mayfield's home was searched with the approval of a federal judge because the available information, including an erroneous finger-print match, gave investigators probable cause to believe that he was involved in the terrorist bombings in Madrid - - the search was not on account of any new authority created by the USA PATRIOT Act or any abuse of the Act.

The ACLU's allegation regarding Mr. Mayfield seems to be based in part on the mistaken idea that the search of Mr. Mayfield's home was conducted pursuant to section 213 of the USA PATRIOT Act. That is not correct. The search was conducted pursuant to the Foreign Intelligence Surveillance Act under an authority that has existed in the FISA statute since 1995. Because the search was conducted under a FISA Court order, some of the USA PATRIOT Act provisions that amended FISA or relate to intelligence investigations may have been implicated or "used" in some sense of that word. That does not in any way mean that these USA PATRIOT Act provisions were misused. The Department would be happy to share other information from

our letter to Senator Feinstein with the Committee.

Moreover, last month, the Department of Justice's Inspector General, Glenn A. Fine, testified before the Subcommittee on Crime, Terrorism and Homeland Security about section 1001 of the USA PATRIOT Act, which directs his office to undertake a series of actions related to complaints of civil rights or civil liberties violations allegedly committed by DOJ employees. In his testimony, Mr. Fine noted that, with the exception of the Brandon Mayfield case, none of the allegations received by his office alleging misconduct by a Department employee related to use of a provision of Patriot Act. That is a significant finding.

Conclusion

Mr. Chairman, I'd like to say a final word about congressional oversight and my concern that Congress, while reauthorizing the USA PATRIOT Act, may seek to include new sunsets. In just the last few weeks, the Attorney General and I have met with dozens of Members of Congress to discuss these important tools. In addition, the Attorney General has appeared three times to testify. Moreover, 32 Department of Justice witnesses have appeared at 17 Congressional hearings which have explored in depth the various tools contained in the USA PATRIOT Act. All of this activity is because Congress is rightly engaging in its critical role to conduct appropriate oversight. But sunsets are not required to conduct oversight. Congress maintains its authority and responsibility to conduct oversight, to ask questions, to demand answers, even without sunsets. My concern is that sunsets on these important tools might inhibit the culture of information sharing that we are trying to foster. Rather than encouraging and empowering our agents and prosecutors to rely upon these new tools, we send a message that a particular provision may only be temporary and chill development of the culture of information sharing. As long as congressional oversight remains robust, which I am convinced it will, there is no need for sunsets.

Mr. Chairman, again, thank you for the opportunity to appear before you today and thanks to you and all your colleagues for providing us with the important tools of the USA PATRIOT Act. I would now be happy to answer any questions.